# Zapory sieciowe

*Materiały pomocnicze do wykładu*

**Bezpieczeństwo systemów informatycznych**

Zapory sieciowe
(*firewalls*)



## Podstawowe funkcje zapory

- Blokowanie dostępu
- Monitorowanie komunikacji
- Podsłuchiwanie i rejestrowanie
- Tunelowanie (*Virtual Private Network*).
- Uwierzytelnianie

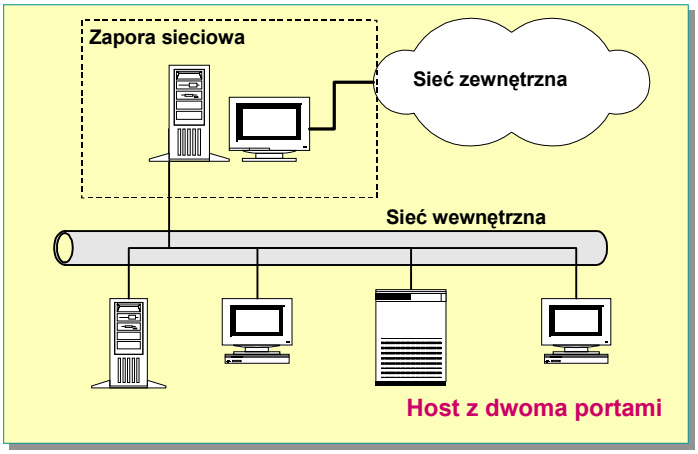


## Podstawowe mechanizmy zapory

- Filtrowanie pakietów
  (*packet filtering*)
- Translacja adresów
  (*network address translations*)
- Usługi proxy
  (*proxy serwers*)

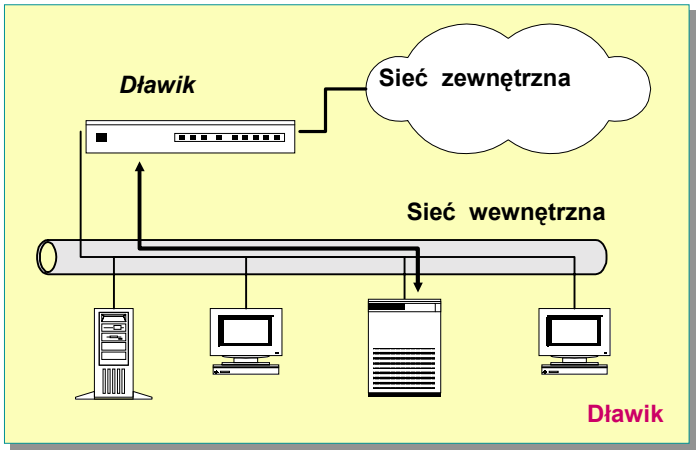


## Tradycyjne konfiguracje zapory

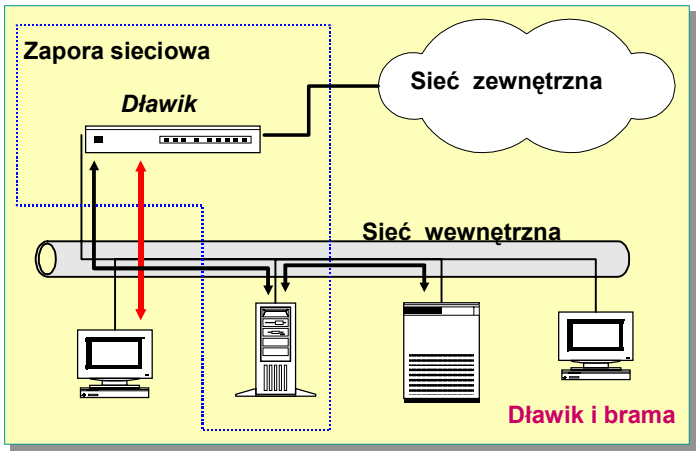





## Tradycyjne konfiguracje zapory

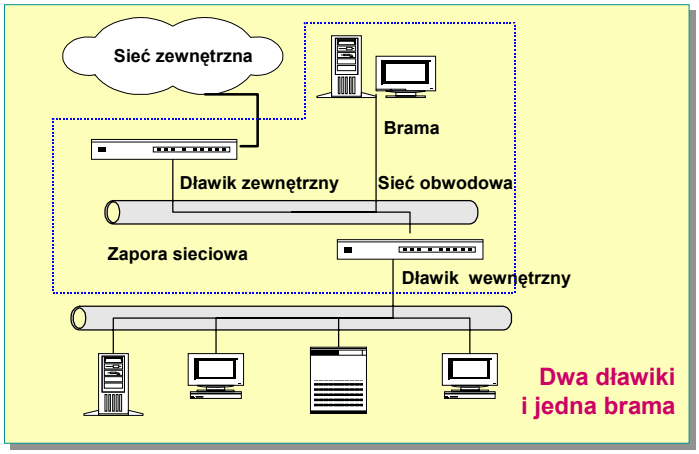


## Tradycyjne konfiguracje zapory



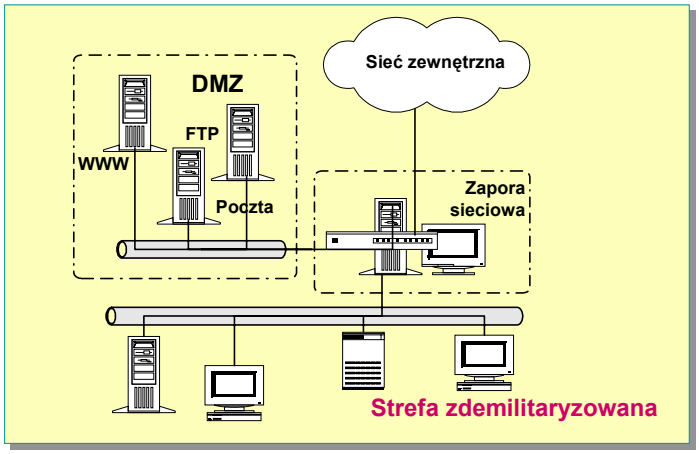



## Tradycyjne konfiguracje zapory






## Tradycyjne konfiguracje zapory



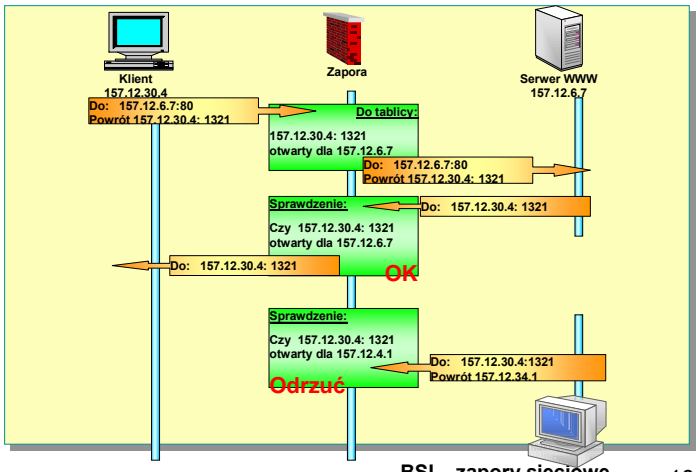



## Filtrowanie bezstanowe

- Filtrowanie adresów IP
- Filtrowanie portów
  - *Telnet,*
  - *NetBIOS Session*
  - *POP*
  - *NFS*
  - *X Windows.*
- Routing źródłowy
- Fragmentacja

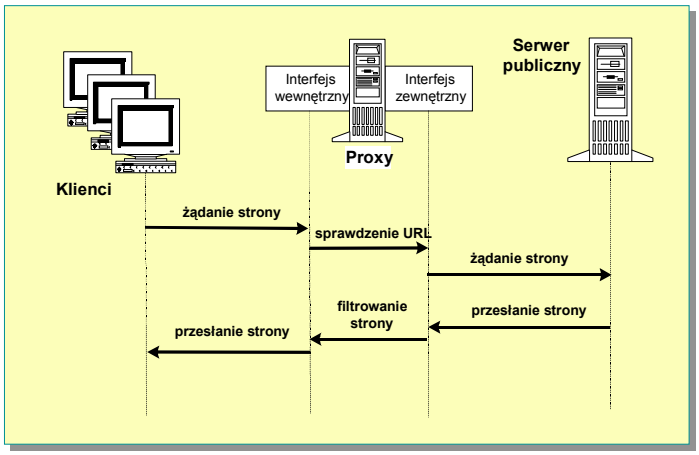


## Filtrowanie z badaniem stanu






## Usługi *PROXY*



## Zalety *PROXY*

- Ukrywanie klienta przed światem zewnętrznym
- Blokowanie niebezpiecznych URL
- Filtrowanie niebezpiecznej zawartości
  (wirusy, konie trojańskie)
- Badanie spójności przesyłanej informacji
- Eliminacja *routingu* między sieciami
- Zapewnienie pojedynczego punktu dostępu
  (nadzorowanie i rejestracja zdarzeń)

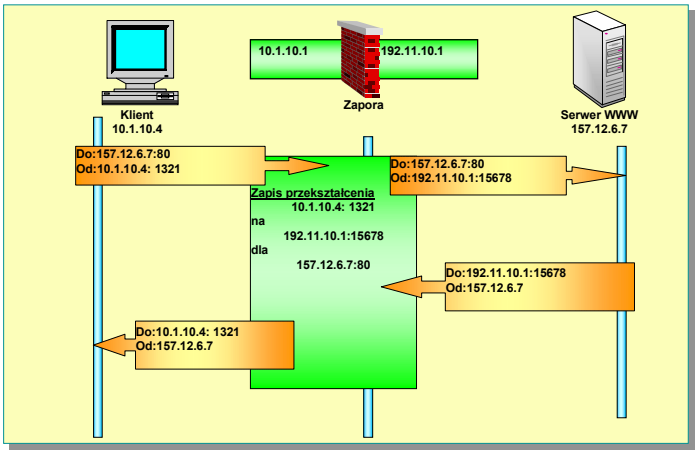


## Wady *PROXY*

- Pojedynczy punkt - wrażliwość na awarie
- Oprogramowanie klienckie musi współpracować z *proxy*
- Każda usługa musi mieć *proxy*
- *Proxy* nie chroni systemu operacyjnego
- Małe bezpieczeństwo konfiguracji domyślnych
- Zatory



## Translacja adresów (NAT)






## Translacja adresów (NAT)

- Translacja statyczna
  (*static translation*)
- Translacja dynamiczna
  (*dynamic translation*)
- Translacja ze zrównoważonym obciążeniem
  (*load balancing translation*)
- Translacja ze zwielokrotnionymi połączeniami
  (*network redundancy translation*)



## Etapy budowy zapory sieciowej

- Planowanie konfiguracji
  - Co chronić ?
  - Jaka jest topologia ?
  - Jakie są potrzeby w zakresie aplikacji i protokołów?
  - Jakie są zależności służbowe ?
  - Jaka powinna być konfiguracja zapory ?
  - Kupić czy budować ?
- Zdefiniowanie reguł dostępu do zasobów sieciowych
- Znalezienie odpowiedniej zapory
- Instalacja i konfiguracja zapory
- Drobiazgowe testowanie zapory